REMARKS/ARGUMENTS

Claim Amendments

The Applicant has amended claims 22-32 to correct the mis-numbering and claims 15 and 18 to correct antecedence errors. Applicant respectfully submits no new matter has been added. Accordingly, claims 1-31 are pending in the application. Favorable reconsideration of the application is respectfully requested in view of the foregoing amendments and the following remarks.

Examiner Objections – Specification

The specification was objected to because of an informality. The Applicant thanks the Examiner for the careful review of the specification. In response, the Applicant has modified the specification as suggested by the Examiner.

Examiner Objections - Claims

Claims 22-32 were objected to because they were misnumbered. The examiner has renumbered to 21 -31. Again, the Applicant appreciates the Examiner's thorough review of the claims.

Claim Rejections – 35 U.S.C. § 102(b)

Claims 1, 2, and 4 stand rejected under 35 U.S.C. 102(b) as being anticipated by Franks J et al (RFC 2069-An Extension to HTTP: Digest Access Authentication). The Applicants respectfully traverse the rejection of these claims.

The Applicant's application points out that an HTTP Digest Authentication method capable of generating a password, according to RFC 3310. However, this method does not provide for delegating a password to a third party application server. Also the Digest authentication method assumes re-generation of a password at each new request. In contrast, the present invention provides a method for generating a password and for delegating the password to a third party application. Particularly, the present invention includes an authentication server capable of generating a password and a third party application server capable of generating a temporary identity for a

user. The application server is further capable of obtaining a password from the authentication server for authenticating the user.

The Franks reference provides an improvement of the basic protocol, HTTP/1.0 (RFC 1945). The user name and password are not passed over the network in an unencrypted format. Frank discloses a scheme (Digest Access Authentication) that verifies that both parties to a communication know a shared secret (a password) (Franks abstract). The Franks verification can be done without sending the password in the clear, which is the basic protocol's biggest weakness.

The Franks reference does not disclose generating a new or different password in the authentication server, Franks merely provides a checksum that includes the username and the original password. Franks does, however, disclose that to authenticate a user, a digest challenge is generated. But, it does not follow that the algorithm for the operation is capable of generating end-user passwords. In fact, the Franks reference assumes that generation of a password has already occurred and is distributed to participating parties after performing mutual authentication. Franks does not disclose generation of a temporary identity for the UE and a password at the UE based on the HTTP Digest challenge. This being the case, the Franks reference does not disclose all the limitations of claim 1.

Claims 2 and 4 depend from claim 1 and recite further limitations in combination with the novel elements of claim 1. The Applicant respectfully requests the allowance of claims 1, 2 and 4.

Claim Rejections – 35 U.S.C. § 103 (a)

Claims 3, and 15-21 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Franks J et al (RFC 2069-An Extension to HTTP: Digest Access Authentication) as applied to claim 1 above, in view of Niemi, et al. (RFC, HTTP Digest Authentication Using AKA). The Applicant respectfully traverses the rejection of these claims.

The Niemi reference discloses the underlying digest authentication method for creating a challenge in the method in the Franks reference. The Applicant has reviewed

the cited portions of Niemi. The Applicant respectfully submits that the portion of Niemi that is purported to disclose sending the identity of the remote server to the authentication node, is merely a definition of 'nonce'. Furthermore, the applicant notes when a client receives a Digest AKA authentication challenge, the resulting AKA RES parameter is treated as "password". This is not a password in the sense of the present application. The Applicant respectfully submits that the Niemi reference does not supply the limitations missing from the Franks reference with regards to claim 1; that of providing a generation of a temporary identity for the UE and a password at the UE based on the HTTP Digest challenge. Claim 3 depends from claim 1 and claim 15 is an analogous independent claim containing similar limitations to claim 1. This being the case the Applicant respectfully submits that the claims 3 and 15-21 are patentable over a combination of the Franks and Niemi references.

Claims 10, and 12-14 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Franks et al (RFC 2069-An Extension to HTTP: Digest Access Authentication) as applied to claims 9 and 15 above, in view of Kadyk, et al. (US 6,996,841 B2), and further in view of Niemi et al (RFC, HTTP Digest Authentication Using AKA). The Applicant respectfully traverses the rejection of these claims.

The Kadyk reference is cited for disclosing the HTTP digest challenge being generated at the authentication node and sent from the authentication node directly to the UE. Claim 10 reads, in part, "...challenge is generated at the authentication node and sent from the authentication node to the remote server ...." The Applicant has reviewed the cited portion of Kadyk and respectfully disagrees with the interpretation of the cited portion. The cited portion of Kadyk describes authenticating a user at a client which includes the steps of a proxy issuing an authenticate challenge, and the client sending proper authentication credentials to the proxy. The Applicant respectfully submits that Niemi and Franks lack limitations that Kadyk does not supply and, this being the case, claims 10 and 12-14 are patentable over the combination of the prior art references of Franks, Niemi and Kadyk.

Claims 22-31 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Franks et al (RFC 2069-An Extension to HTTP: Digest Access Authentication) as applied to claim 1 and 15 above, in view of Niemi, et al. (RFC, HTTP Digest Authentication Using AKA), and further in view of Kadyk, et al. (US 6,996,841 B2). The Applicant respectfully traverses the rejection of these claims.

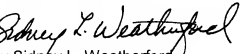
Claims 22-31 depend from claim 15 and contain the same limitations. The combination of Franks, Niemi and Kadyk lack the limitations present in claims 1 and 15, as noted above. This being the case, the applicant respectfully submits that claims 22-31 are patentable over the Niemi, Franks and Kadyk references.

CONCLUSION

In view of the foregoing remarks, the Applicant believes all of the claims currently pending in the Application to be in a condition for allowance. The Applicant, therefore, respectfully requests that the Examiner withdraw all rejections and issue a Notice of Allowance for all pending claims.

The Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,



By Sidney L. Weatherford
Registration No. 45,602

Date: April 17, 2008

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024
(972) 583-8656
sidney.weatherford@ericsson.com